

WHAT IS CLAIMED IS:

1. The use of an optical disc, commonly referred to as "Compact Disc" or Digital Versatile Disc" that contains an embedded and encrypted digital signature for the use of signing legal and financial transactions over a networked environment or over the Internet.

2. The storage of a digital signature or digital certificate on a CD-ROM, CD-R, CD-RW or DVD disc for purpose of making the digital signature portable for use on several different computers without expert knowledge in the field of digital certificates.

3. The storage of a digital signature on a compact or DVD disc in encrypted form for the reasons of providing security.

4. The use of more than one digital signature on a single disc for the purpose of providing new digital signatures on a rotating or annual basis.

5. The use of more than one digital signature on a single disc for the purpose of providing immediately available additional digital signatures in the event that the current digital signature is compromised and can no longer be used in a secure manner.

6. The method of incorporating the date as part of the encryption key for protecting the digital signature. The date is added as a portion of the password or pass phrase to form a new password. The new unique password or pass phrase is then used to decrypt a new digital signature. The date can appear as either some numeric form of the date or as an obscured pass phrase or worded term.

7. The use of a software module to decrypt the digital signature contained on a compact disc or other form of media in a manner such that secure data to access the digital signature is entered and processed locally without allowing the entered password or pass phrase to leave the local computer memory.

8. The use of downloadable software components for the purpose of decrypting the digital signature. The source of the software components may be provided locally by residing on the disc containing the digital signature, as part of a third party software package or provided from a remote computer via a network environment.

9. The use of downloadable software components for the specific purpose of aging the digital signature or certificate with or without the user's knowledge. Such components would seek out the next available digital signature or certificate on an automatic basis.



